PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-337736
(43)Date of publication of application : 28.11.2003

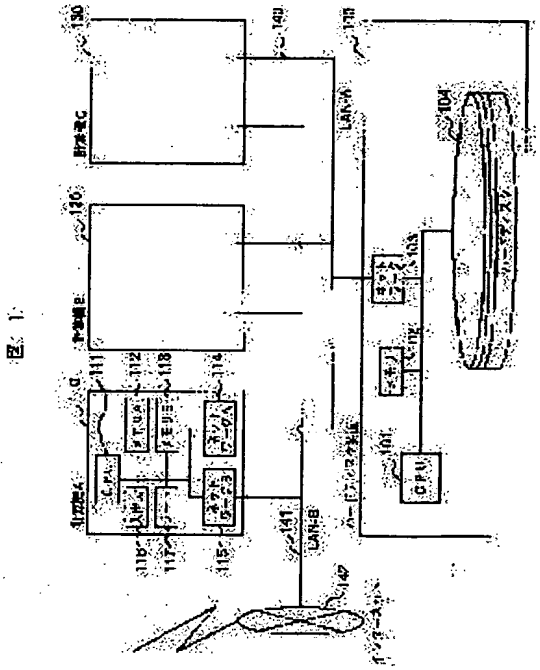
(51)Int.CI. G06F 12/00
G06F 3/06
G06F 12/14
H04L 9/10

(21)Application number : 2002-144942
(22)Date of filing : 20.05.2002

(71)Applicant : HITACHI LTD
(72)Inventor : KIMURA SHINJI
KARASAKI SADAJI
SATO MASAHIDE
OSHIMA SATOSHI

(54) COMPUTER, HARD DISK DEVICE, DISK DEVICE SHARING SYSTEM CONSTRUCTED OF A PLURALITY OF COMPUTERS AND SHARED HARD DISK DEVICE, AND SHARING METHOD FOR DISK DEVICE USED IN THE SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To realize safety data communication between respective computers and a shared hard disk device mutually connected via a network and to provide a disk device sharing system reducing the operation cost required for maintenance of the computers.
SOLUTION: Two OS are mounted on a single computer. One is a first OS executing an application program, while the other is a second OS processing communication with the shared hard disk device. Access from the application program to the shared hard disk device is always passed through the second OS, and control is carried out so that direct access from the application program and the first OS to the hard disk device is not allowed.



LEGAL STATUS

[Date of request for examination] 13.07.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－337736
（P2003－337736A）
(43)公開日　平成15年11月28日(2003.11.28)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)
G06F	12/00	545	G06F	12/00	545A　5B017
		537			537H　5B065
	3/06	301		3/06	301C　5B082
		304			304H　5J104
	12/14	320		12/14	320A

審査請求　未請求　請求項の数20　ＯＬ　（全 12 頁）　最終頁に続く

(21)出願番号　特願2002－144942(P2002－144942)

(22)出願日　平成14年５月20日(2002.5.20)

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　木村　信二
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　唐崎　貞二
神奈川県海老名市下今泉810番地　株式会社日立製作所インターネットプラットフォーム事業部内
(74)代理人　100068504
弁理士　小川　勝男　（外２名）

最終頁に続く

(54)【発明の名称】　計算機、ハードディスク装置、複数の該計算機及び共有ハードディスク装置から構成されるディスク装置共有システム、及び該共有システムにおいて利用されるディスク装置の共有方法

(57)【要約】
【課題】　複数の計算機と共有ハードディスク装置がネットワークで相互接続される環境において、各計算機とハードディスク装置間の安全なデータ通信を実現し、計算機用のメンテナンスに要する運用コストの低減するディスク装置共有システムを提供する。
【解決手段】　１台の計算機上に２つのＯＳを搭載する。１つは、アプリケーションプログラムを実行する第一のＯＳ、もう一つは共有するハードディスク装置との通信処理を行う第２のＯＳである。アプリケーションプログラムからの共有ハードディスク装置へのアクセスは、必ず第二のＯＳを経由させ、アプリケーションプログラム及び第一のＯＳからはハードディスク装置に直接アクセスできないよう制御する。

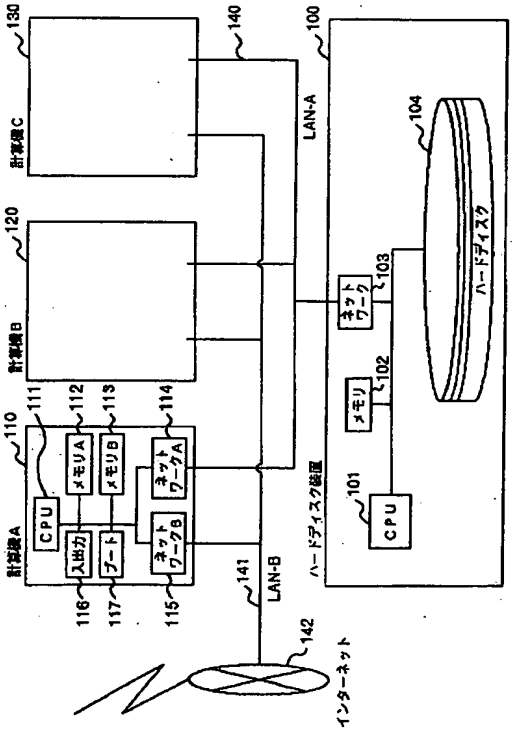


図１

【特許請求の範囲】

【請求項１】アプリケーションプログラムを実行する複数の計算機と、前記複数の計算機により共用されるハードディスク装置と、前記複数の計算機と前記ハードディスク装置がネットワークにより相互接続されるディスク装置共有システムにおいて、

前記複数の計算機は、前記アプリケーションプログラムを実行する第１のオペレーティングシステムと、前記計算機と前記ハードディスク装置間の通信処理を実施する第２のオペレーティングシステムとを備え、前記第１のオペレーティングシステムと第２のオペレーティングシステムとは相互に独立して実行することを特徴とするディスク装置共有システム。

【請求項２】前記第１のオペレーティングシステムは前記計算機においてユーザにより実行される前記アプリケーションプログラムを制御するユーザ処理ＯＳであり、前記第２のオペレーティングシステムは、前記計算機と前記ハードディスク装置間の通信処理を制御する通信処理ＯＳであり、前記複数の計算機は、内臓ディスクを備えないことを特徴とする請求項１に記載のディスク装置共有システム。

【請求項３】前記ハードディスク装置は、鍵生成データを備え、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化することを特徴とする請求項２に記載のディスク装置共有システム。

【請求項４】請求項３記載のディスク装置共有システムにおいて、

前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第１のオペレーティングシステム、第２のオペレーティングシステム、及び前記アプリケーションプログラムをプログラムブートすることを特徴とする請求項３に記載のディスク装置共有システム。

【請求項５】前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第１のオペレーティングシステム及び第２のオペレーティングシステムをプログラムブートし、前記アプリケーションプログラムをデータとして、前記ハードディスク装置からロードすることを特徴とする請求項３に記載のディスク装置共有システム。

【請求項６】前記ハードディスク装置は、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化するために、前記鍵生成データに基づき鍵データを作成し、前記プログラムブート時に前記複数の計算機に対し前記鍵生成データ、或いは前記鍵データを配信することを特徴とする請求項５に記載のディスク装置共有システム。

【請求項７】第１のＯＳと第２のＯＳを備えた計算機から構成され、該第１のＯＳと第２のＯＳは相互に独立して実行し、前記計算機はユーザにより利用されるアプリケーションソフト及び通信処理部を備え、前記ユーザが前記第１のＯＳの制御により前記アプリケーションソフトを実行した結果、得られるデータを前記通信処理部が備える暗号処理ユニットにて前記第２のＯＳの制御により暗号化し、前記第２のＯＳにより制御されるネットワーク部を介して前記暗号化されたデータを外部インターフェースに接続されるハードディスク装置に送信することを特徴とする計算機。

【請求項８】請求項７記載の計算機において、

前記第２のＯＳは前記通信処理部を制御し、前記暗号処理ユニットは前記ハードディスク装置から配信された鍵生成データに基づき鍵データを作成し、前記データの前記暗号化を実施することを特徴とする計算機。

【請求項９】請求項８記載の計算機において、

前記第１のＯＳは前記アプリケーションソフトを制御するユーザ処理ＯＳであり、前記第２のＯＳは前記ネットワーク部を介して前記ハードディスク装置と前記暗号化された前記データの通信を実施する通信処理ＯＳであることを特徴とする計算機。

【請求項１０】ＣＰＵ、メモリ、ハードディスクユニット及びネットワーク部を備えるハードディスク装置から構成され、

前記ＣＰＵはブート処理部、認証プログラムユニット、通信処理部及び前記ハードディスクユニットを制御するディスク管理部を含み、

前記通信処理部は、暗号処理ユニット及び鍵生成データを備え、

前記認証プログラムユニットは前記ネットワーク部を介して接続されている複数の計算機の各々が有するハードウェア情報及び前記計算機を管理する使用者情報を保持し、

前記ハードディスクユニットは複数の領域を備え、該複数の領域には前記複数の計算機毎の前記ハードウェア情報が格納され、

前記暗号処理ユニットは、前記計算機から送信されるブート要求を前記ブート処理部にて処理した後、前記鍵生成データに基づき鍵データを作成し、前記ハードウェア情報に前記鍵生成データ或いは鍵データを付加して前記ブート要求を発信した前記計算機に対し配信することを特徴とするハードディスク装置。

【請求項１１】請求項１０記載のハードディスク装置において、

前記ハードウェア情報は前記計算機毎に格納されているユーザ処理ＯＳ、通信処理ＯＳ、及びユーザにより利用されるアプリケーションプログラムを含み、前記使用者情報はユーザを識別する為の認証情報であることを特徴とするハードディスク装置。

【請求項１２】請求項１１記載のハードディスク装置において、

前記認証情報は、前記計算機を使用するユーザ名、該ユ

ーザのパスワード、及び該ユーザが利用しているデータ格納用ディスクの情報であることを特徴とするハードディスク装置。

【請求項１３】請求項１０記載のハードディスク装置において、

前記鍵データは前記暗号処理ユニットが備える鍵データ部において作成され、前記鍵データ部は計算機を識別する為の固有データ及び暗号化情報を保持することを特徴とするハードディスク装置。

【請求項１４】請求項１３記載のハードディスク装置において、

前記固有データ及び暗号化情報は前記計算機のネットワークアドレス、前記鍵生成データ、前記鍵データ、及び前記鍵データの生成時間を含む情報であることを特徴とするハードディスク装置。

【請求項１５】請求項１０記載のハードディスク装置において、

前記ディスク管理部の制御に従い、前記計算機から前記送信される暗号化された通信データを前記通信処理部が処理し、前記ハードディスクユニットが有する前記複数の領域の内、何れかの領域に前記暗号化された通信データを格納することを特徴とするハードディスク装置。

【請求項１６】請求項１５記載のハードディスク装置において、

さらに、前記ディスク管理部の制御に従い、前記計算機から送信される前記暗号化された通信データを前記暗号処理ユニットが有する前記鍵データを使用し、暗号化されていない元データに戻し、前記複数の領域の内、何れかの領域に該元データを格納することを特徴とするハードディスク装置。

【請求項１７】複数の計算機と、該複数の計算機により共用されるハードディスク装置と、該複数の計算機と前記ハードディスク装置がネットワークにより相互接続される計算機システムにおいて、

前記計算機システムがブート処理するステップと、

前記ブート処理の後、前記計算機はユーザによる認証ＩＤの入力後、認証データを作成し前記ハードディスク装置に対し、送信するステップと、

前記ハードディスク装置にて前記認証データの認証処理を実施し、前記複数の計算機に対し、前記ハードディスク装置が備える暗号処理部が鍵データを作成するステップと、

前記計算機の実行に必要と成るオペレーティングシステム、前記ユーザにより利用されるアプリケーションソフトと共に前記鍵データを前記計算機に対し配信するステップとを含むことを特徴とするディスク装置の共有方法。

【請求項１８】請求項１７記載のディスク装置の共有方法において、

前記ハードディスク装置は、鍵生成データ及び鍵データ部を備え、前記作成するステップにおいて、前記鍵生成データに基づいて前記鍵データが作成され、前記鍵データ部は前記複数の計算機と前記ハードディスク装置間の通信データを前記暗号処理部にて暗号化する際に必要な前記鍵データを格納することを特徴とするディスク装置の共有方法。

【請求項１９】請求項１８記載のディスク装置の共有方法において、

前記オペレーティングシステムは、ユーザ処理ＯＳ及び通信処理ＯＳを含み、前記配信するステップにおいて、前記計算機に対し、前記鍵生成データ或いは鍵データが前記オペレーティングシステム及びアプリケーションソフトと共に送信されることを特徴とするディスク装置の共有方法。

【請求項２０】請求項１７記載のディスク装置の共有方法において、

さらに前記鍵データを用いて、前記計算機は前記ユーザにより利用されるアプリケーションソフトを実行した結果、得られるデータを暗号化し前記ハードディスク装置に対し前記ネットワークを介して転送するステップを含むことを特徴とするディスク装置の共有方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、複数の計算機がハードディスク装置を共有するディスク装置共有システムに関し、特に、該共有システムにおいて利用される当該ディスク装置の共有方法に関する。

【０００２】

【従来の技術】計算機は使用する形態により分類できるが、ユーザが文書処理等のアプリケーションプログラムで使用するパソコン等の計算機はクライアント計算機、また、Ｗｅｂサーバやメールサーバのように複数のユーザにサービスを提供するためのアプリケーションプログラムを実行する計算機はサーバ計算機と呼ばれる。

【０００３】このようなクライアント計算機やサーバ計算機は、基本的な構成は同じであり、高性能なＣＰＵ、大容量のメモリ、大容量なハードディスク装置、及び高速なグラフィック装置等を搭載している。オペレーティングシステム（ＯＳ）、アプリケーションプログラムやユーザデータ等はストレージとしてのハードディスク装置に格納される。

【０００４】また、ネットワークコンピュータと呼ばれる計算機の形態があるが、これは、ＯＳやアプリケーションプログラムを格納するハードディスク装置を各クライアント計算機に備えず、サーバ計算機上でアプリケーションプログラムを実行し、その表示のみの機能を備えることによって、低価格、低機能化した計算機である。

【０００５】また、複数の計算機でハードディスク装置を共有する方法として、Ｅｔｈｅｒｎｅｔ（登録商標）のようなネットワーク上の通信プロトコルに、ハードデ

ィスク装置にアクセスするためのＳＣＳＩプロトコルを使う、ｉＳＣＳＩ（Ｉｎｔｅｒｎｅｔ Ｓｍａｌｌ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍｓ Ｉｎｔｅｒｆａｃｅ）プロトコルが知られている。

【０００６】計算機がプリブート／リモートブート機能を備える場合は、ＯＳやアプリケーションプログラムのロードを、サーバ計算機から行えるため、前記ｉＳＣＳＩプロトコルを使ったハードディスク装置の共有と組み合わせることによって、各計算機にハードディスク装置を備える必要のない計算機を実現できる。このような計算機はディスクレス計算機と呼ばれる。

【０００７】

【発明が解決しようとする課題】上述したディスクレス計算機は、ＯＳ、アプリケーションプログラム及びユーザデータを、ネットワークにより共有したハードディスク装置に格納できるためのインストール、バージョンアップ、バックアップに伴う作業を簡素化できる利点がある。

【０００８】しかし、Ｅｔｈｅｒｎｅｔ（登録商標）のようなネットワークを使用して、計算機とストレージを接続する形態では、ネットワーク上のデータは盗聴可能であり安全でないという問題がある。ここで、盗聴とはハッカー等によるデータの改変の事である。

【０００９】また、複数のディスクレス計算機と共有ハードディスク装置がネットワークで接続される形態では、１台のディスクレス計算機の管理者権限が奪われると、同じネットワーク上の計算機及びハードディスク装置内におけるデータの安全性が失われるという問題がある。

【００１０】本発明の目的は、複数の計算機と共有ハードディスク装置がネットワークを介して相互接続される環境において、安全なデータ通信を実現し、計算機のメンテナンスに要する運用コストの低減を実現するディスク装置共有システムを提供する事にある。

【００１１】

【課題を解決するための手段】前記課題を解決し、上述した目的を達成するために、本発明は１台の計算機上に２つのＯＳを搭載する。１つは、アプリケーションプログラムを実行する第一のＯＳ、もう一つは共有するハードディスク装置との通信処理を行う第２のＯＳである。本発明によれば、アプリケーションプログラムを実行する第一のＯＳの管理者権限を不正なプログラムにより奪われても、第２のＯＳの管理者権限を奪わなければ、共有ハードディスク装置にアクセスすることはできない。

【００１２】さらに、本発明によれば、第２のＯＳと共有ハードディスク装置間の通信データを暗号化することによって、他の計算機からのデータ盗聴を防ぐことが可能になる。各計算機のＯＳをプリブート／リモートブート機能を使って、共有ハードディスク装置から配布するときに、通信データの暗号化に必要な鍵データを、リモートブートするＯＳといっしょに配布することによって、各計算機に鍵データを保存する必要がないため、鍵データの盗難を防ぐことが可能である。

【００１３】さらに、配布する鍵データは第２のＯＳが管理するメモリ領域に保存し、第１のＯＳからアクセスできないようにすることによって、安全性を高めることができる。

【００１４】

【発明の実施の形態】本発明の実施の形態について説明する。尚、実施例を示す各図における同一符号は同一物または相当物を示す。以下、図面を用いて本発明の実施の形態について説明する。図１は本発明の実施の形態におけるディスク装置共有システムを使用した計算機環境の構成を示す図である。

【００１５】ハードディスク装置１００は、計算機Ａ１１０、計算機Ｂ１２０、計算機Ｃ１３０のＯＳ、アプリケーションプログラム及びユーザデータを格納するための共有ハードディスク装置である。当該ハードディスク装置はＣＰＵ１０１、メモリ１０２、ネットワークデバイス１０３及び、ハードディスクデバイス１０４で構成される。ハードディスクデバイス１０４には、各使用者のＯＳ、アプリケーションプログラム及びユーザデータが格納されているものとする。

【００１６】計算機Ａ１１０、計算機Ｂ１２０、計算機Ｃ１３０は使用者Ａ、Ｂ、Ｃが使用する計算機である。それぞれの計算機は、ＣＰＵ１１１、メモリＡ１１２、メモリＢ１１３、ネットワークデバイスＡ１１４、ネットワークデバイスＢ１１５、入出力デバイス１１６、ブート制御回路１１７から構成される。各計算機に内蔵されているネットワークデバイスＡ１１４は、ＬＡＮ－Ａ１４０を経由して、ハードディスク装置１００に接続される。また、ネットワークデバイスＢ１１５はＬＡＮ－Ｂ１４１を経由して、インターネット１４２に接続されているものとする。また、入出力デバイス１１６は、キーボードと表示装置で構成されるものとする。

【００１７】本発明の実施形態による図１に示すディスク装置共有システムは、以下の項目（ａ）から（ｆ）の特徴を有するディスク装置共有システムとして提供することも可能である。

【００１８】（ａ）アプリケーションプログラムを実行する複数の計算機と、前記複数の計算機により共用されるハードディスク装置と、前記複数の計算機と前記ハードディスク装置がネットワークにより相互接続されるディスク装置共有システムにおいて、前記複数の計算機は、前記アプリケーションプログラムを実行する第１のオペレーティングシステムと、前記計算機と前記ハードディスク装置間の通信処理を実施する第２のオペレーティングシステムとを備え、前記第１のオペレーティングシステムと第２のオペレーティングシステムとは相互に独立して実行することを特徴とするディスク装置共有シ

ステム。

【００１９】（ｂ）前記第１のオペレーティングシステムは前記計算機においてユーザにより実行される前記アプリケーションプログラムを制御するユーザ処理ＯＳであり、前記第２のオペレーティングシステムは、前記計算機と前記ハードディスク装置間の通信処理を制御する通信処理ＯＳであり、前記複数の計算機は、内臓ディスクを備えないことを特徴とする、上記（ａ）に記載のディスク装置共有システム。

【００２０】（ｃ）前記ハードディスク装置は、鍵生成データを備え、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化することを特徴とする、上記（ｂ）に記載のディスク装置共有システム。

【００２１】（ｄ）前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第１のオペレーティングシステム、第２のオペレーティングシステム、及び前記アプリケーションプログラムをプログラムブートすることを特徴とする、上記（ｃ）に記載のディスク装置共有システム。

【００２２】（ｅ）前記複数の計算機は、前記ネットワークを経由して前記ハードディスク装置から前記第１のオペレーティングシステム及び第２のオペレーティングシステムをプログラムブートし、前記アプリケーションプログラムをデータとして、前記ハードディスク装置からロードすることを特徴とする、上記（ｃ）に記載のディスク装置共有システム。

【００２３】（ｆ）前記ハードディスク装置は、前記複数の計算機と前記ハードディスク装置間の通信データを暗号化するために、前記鍵生成データに基づき鍵データを作成し、前記プログラムブート時に前記複数の計算機に対し前記鍵生成データ、或いは前記鍵データを配信することを特徴とする、上記（ｅ）に記載のディスク装置共有システム。

【００２４】図２は本発明の実施の形態における図１の計算機Ａ１１０、計算機Ｂ１２０、計算機Ｃ１３０で動作するソフトウェアの構成を示したものである。

【００２５】各計算機では、使用者が使用するアプリケーションプログラム２０４を実行するユーザ処理ＯＳ２００と、ハードディスク装置１００との通信を処理する通信処理ＯＳ２０１とが独立して実行する。独立して実行するとは、２つのＯＳが計算機１１０、１２０、１３０の資源であるメモリや入出力デバイスを分割して利用し、互いの実行が他に影響を与えないことを言う。この複数のＯＳを実行するための処理は複数ＯＳ処理２０２で行う。１つの計算機で複数のＯＳを独立に実行する技術は、特開平１１－１４９３８５号公報（以下、文献１と称する）に開示されている。上記文献１によれば、ユーザ処理ＯＳ２００と通信処理ＯＳ２０１を独立実行でき、ユーザ処理ＯＳ２００が障害で停止した場合でも、通信処理ＯＳ２０１は継続して動作できる。

【００２６】ユーザ処理ＯＳ２００は、ＬＡＮ－Ｂ１４１を経由してインターネットに接続するためのネットワーク処理２０６と、アプリケーションプログラム２０４からのディスク装置へのアクセスを行う際、ディスク装置に対し、通常、送信する制御コマンドなどを通信プロトコルに変換するための仮想ディスク処理２０７を備える。仮想ディスク処理２０７は、複数ＯＳ処理２０２が提供するＯＳ間通信処理２０３を使い、もうひとつのＯＳ２０１で実行される通信処理２０５に通信データを送る。通信処理２０５は、必要に応じて、暗号処理２０９で通信データの暗号化を行い、通信処理ＯＳ２０１のネットワーク処理２０８によりＬＡＮ－Ａ１４０を経由して、ハードディスク装置１００と通信処理を行う。計算機１１０、１２０、１３０とハードディスク装置１００の通信データを暗号化する場合は、メモリＡ１１２（図１）に格納した鍵生成データ２１０から求めた鍵データ２１１を用いて暗号化した通信データで通信を行うものとする。ここで、上述した通信データの暗号化は、公開暗号鍵方式に準拠している。通信処理ＯＳ２０１、複数ＯＳ処理２０３、鍵生成データ２１０はメモリＡ１１２に格納され、ユーザ処理ＯＳ２００はメモリＢ１１３に格納する。これらの処理ソフトウェア及びデータは、計算機１１０、１２０、１３０の電源を入れたときに、ブート制御回路１１７に格納されたプリブート／リモートブート機能により、ネットワークデバイスＡ１１４を使い、ＬＡＮ－Ａ１４０を経由して、ハードディスク１００からネットワークブートによりロードされる。

【００２７】本発明の図２に示すソフトウェアの構成に基づき、動作する図１の各計算機Ａ１１０、Ｂ１２０、Ｃ１３０は、以下の項目（Ｉ）から（ＩＩＩ）の特徴を有する計算機として提供することも可能である。

【００２８】（Ｉ）第１のＯＳと第２のＯＳを備えた計算機から構成され、該第１のＯＳと第２のＯＳは相互に独立して実行し、前記計算機はユーザにより利用されるアプリケーションソフト及び通信処理部を備え、前記ユーザが前記第１のＯＳの制御により前記アプリケーションソフトを実行した結果、得られるデータを前記通信処理部が備える暗号処理ユニットにて前記第２のＯＳの制御により暗号化し、前記第２のＯＳにより制御されるネットワーク部を介して前記暗号化されたデータを外部インターフェースに接続されるハードディスク装置に送信することを特徴とする計算機。

【００２９】（ＩＩ）前記第２のＯＳは前記通信処理部を制御し、前記暗号処理ユニットは前記ハードディスク装置から配信された鍵生成データに基づき鍵データを作成し、前記データの前記暗号化を実施することを特徴とする、上記（Ｉ）に記載の計算機。

【００３０】（ＩＩＩ）前記第１のＯＳは前記アプリケーションソフトを制御するユーザ処理ＯＳであり、前記第２のＯＳは前記ネットワーク部を介して前記ハードデ

ィスク装置と前記暗号化された前記データの通信を実施する通信処理ＯＳであることを特徴とする、上記（ＩＩ）に記載の計算機。

【００３１】図３は本発明の実施の形態におけるハードディスク装置１００で動作するソフトウェアの構成を示したものである。ハードディスク装置１００では、ストレージＯＳ３００が動作する。ストレージＯＳ３００上で、各計算機からのプリブート／リモートブート要求を処理するリモートブート処理３０１、各計算機を使用する使用者の認証を行う認証プログラム３０２、及び、各計算機との通信処理を行う通信処理３０３が動作する。また、ストレージＯＳ３００は、各計算機の実行に必要なプログラムとデータを格納するストレージデバイスを制御するためのディスク管理処理３０５と、ＬＡＮ－Ａ１４０を経由して各計算機と通信を行うためのネットワーク処理３０６を備える。ハードディスクデバイス１０４は、いくつかの領域に分かれている。当該領域において、各計算機をネットワークブートするための、ブートローダプログラム３０７と、使用者毎のＯＳ、アプリケーションプログラムとユーザデータを格納するための領域を有する。使用者Ａ用領域３０８、使用者Ｂ用領域３０９、使用者Ｃ用領域３１０は当該領域に含まれる。

【００３２】また、各ソフトウェア処理は、処理に必要なデータもハードディスクデバイス１０４に格納している。さらに、ハードディスク装置１００内には使用者情報３１１、計算機情報３１２、鍵データ３１３、及びマップ情報３１４が備えられている。使用者情報３１１はハードディスク装置１００に格納されたプログラム／データへのアクセスを認められた使用者を管理する情報である。同様に計算機情報３１２はアクセスを認められた計算機を管理する情報である。鍵データ３１３は各計算機とハードディスク装置１００の間の通信データを暗号処理３０４で暗号化する場合に必要な鍵データを格納する。又、マップ情報３１４はアクセスが認められた使用者／計算機とハードディスクデバイス１０４の領域の対応関係を格納する。

【００３３】本発明の図３に示すソフトウェアの構成に基づき、動作する図１のハードディスク装置１００は、以下の項目（ｉ）から（ｖｉｉ）の特徴を備えるハードディスク装置として提供しうる。

【００３４】（ｉ）ＣＰＵ、メモリ、ハードディスクユニット及びネットワーク部を備えるハードディスク装置から構成され、前記ＣＰＵはブート処理部、認証プログラムユニット、通信処理部及び前記ハードディスクユニットを制御するディスク管理部を含み、前記通信処理部は、暗号処理ユニット及び鍵生成データを備え、前記認証プログラムユニットは前記ネットワーク部を介して接続されている複数の計算機の各々が有するハードウェア情報及び前記計算機を管理する使用者情報を保持し、前記ハードディスクユニットは複数の領域を備え、該複数の領域には前記複数の計算機毎の前記ハードウェア情報が格納され、前記暗号処理ユニットは、前記計算機から送信されるブート要求を前記ブート処理部にて処理した後、前記鍵生成データに基づき鍵データを作成し、前記ハードウェア情報に前記鍵生成データ或いは鍵データを付加して前記ブート要求を発信した前記計算機に対し配信することを特徴とするハードディスク装置。

【００３５】（ｉｉ）前記ハードウェア情報は前記計算機毎に格納されているユーザ処理ＯＳ、通信処理ＯＳ、及びユーザにより利用されるアプリケーションプログラムを含み、前記使用者情報はユーザを識別する為の認証情報であることを特徴とする、上記（ｉ）に記載のハードディスク装置。

【００３６】（ｉｉｉ）前記認証情報は、前記計算機を使用するユーザ名、該ユーザのパスワード、及び該ユーザが利用しているデータ格納用ディスクの情報であることを特徴とする、上記（ｉｉ）に記載のハードディスク装置。

【００３７】（ｉｖ）前記鍵データは前記暗号処理ユニットが備える鍵データ部において作成され、前記鍵データ部は計算機を識別する為の固有データ及び暗号化情報を保持することを特徴とする、上記（ｉ）に記載のハードディスク装置。

【００３８】（ｖ）前記固有データ及び暗号化情報は前記計算機のネットワークアドレス、前記鍵生成データ、前記鍵データ、及び前記鍵データの生成時間を含む情報であることを特徴とする、上記（ｉｖ）に記載のハードディスク装置。

【００３９】（ｖｉ）前記ディスク管理部の制御に従い、前記計算機から前記送信される暗号化された通信データを前記通信処理部が処理し、前記ハードディスクユニットが有する前記複数の領域の内、何れかの領域に前記暗号化された通信データを格納することを特徴とする、上記（ｉ）に記載のハードディスク装置。

【００４０】（ｖｉｉ）さらに、前記ディスク管理部の制御に従い、前記計算機から送信される前記暗号化された通信データを前記暗号処理ユニットが有する前記鍵データを使用し、暗号化されていない元データに戻し、前記複数の領域の内、何れかの領域に該元データを格納することを特徴とする、上記（ｖｉ）に記載のハードディスク装置。

【００４１】図４から図７は、データの構造を示したテーブルである。当該テーブルは、前記ハードディスクデバイス１０４に格納されたハードディスク１００で動作するソフトウェア３００、３０１、３０２、３０３が使用する。ここでソフトウェア３００、３０１、３０２、３０３は各々ストレージＯＳ３００、リモートブート処理３０１、認証プログラム３０２、通信処理３０３に該当する。

【００４２】図４は、使用者情報３１１の詳細を示した

テーブル構造である。使用者情報３１１は、使用者の名前を格納する使用者名４００、使用者を認証するためのパスワード４０１、及び、使用者が割り当てられたハードディスクデバイス１０４の領域を示すデータディスク情報４０２で構成される。

【００４３】図５は、計算機情報３１２の詳細を示したテーブル構造である。計算機情報３１２は、計算機を識別するための名称を格納した計算機名５００、各計算機のネットワークデバイスＡ１１４毎の固有のハードウェア情報であるＭＡＣアドレス５０１、及び、各計算機の構成情報から求めたハードウェア情報５０２で構成される。ハードウェア情報５０２は、各計算機のＣＰＵ１１１のクロック性能とメモリＡ１１２とメモリＢ１１３の搭載メモリサイズの合計値から計算で求めた値を使用するものとする。ここで、ＭＡＣはＭｅｄｉａ．Ａｃｃｅｓｓ　Ｃｏｎｔｒｏｌに該当する。

【００４４】図６は、マップ情報３１４の詳細を示したテーブル構造である。マップ情報３１４は、使用者が使用する計算機と計算機が必要とするハードディスク領域の対応を格納するテーブルである。当該マップ情報３１４は、使用者情報３１１から得られたディスク情報４０２と、計算機情報３１２から得られたＭＡＣアドレス５０１を格納している。

【００４５】図７は鍵データ３１３の詳細を示したテーブル構造である。鍵データ３１３は、各計算機を識別するために、計算機情報３１２から得られるＭＡＣアドレス５０１を格納し、ＭＡＣアドレス５０１毎に鍵データを管理する。鍵データ３１３のテーブルは、暗号化するための鍵データを生成するための鍵生成データ７００を格納する。さらに、鍵生成データ７００から生成し、通信データの暗号化に用いる鍵データ７０１を格納している。そして、鍵データ７０１を生成した生成時間７０２を格納する。鍵生成データ７００は計算機毎に異なる値が設定される。さらに生成した鍵データは生成時間を管理する。又、一定時間ごとに鍵生成データ７００から鍵データ７０１を生成し、暗号化に用いる鍵データを変更することによって、通信データの安全性を高める。

【００４６】図８（ａ）、（ｂ）は、図１に示す各計算機１１０、１２０、１３０とハードディスク装置１００のプログラム起動手順を示すフローチャートである。

【００４７】プログラム起動手順では、まず、計算機１１０、１２０、１３０の電源がオンになると（ステップ８００）、ブート制御回路１１７が起動し、ネットワークデバイスＡ１１４を使用して、ＬＡＮ－Ａ１４０のネットワークに対して、プリブート／リモートブートを要求する（ステップ８０１）。

【００４８】ＬＡＮ－Ａ１４０上のプリブート／リモートブートの要求は、ハードディスク装置１００内のリモートブート処理３０１（図３）が受け付ける。リモートブート処理３０１は、計算機情報３１２を参照し、プリブート／リモートブートを要求している計算機の計算機名５００（図５）とＭＡＣアドレス５０１を比較する（ステップ８０２）。テーブルに格納されている計算機の場合は、ブートローダプログラム３０７を要求元の計算機に送信する（ステップ８０３）。

【００４９】次に、要求元の計算機は、ハードディスク装置１００から送信されたブートローダプログラム３０７を実行し、入出力デバイス１１６により、使用者の使用者名とパスワードを確認する（ステップ８０４）。また、当該計算機は使用者が使用している計算機のＣＰＵ１１１のクロック性能とメモリＡ１１２とメモリＢ１１３の搭載メモリサイズの合計値を組み合わせた値（ハードウェア情報５０２）を計算する（ステップ８０５）。その後、計算機は認証データとして、使用者名、パスワード、ハードウェア情報の３つを、ハードディスク装置１００に送信する（ステップ８０６）。

【００５０】次に、ハードディスク装置１００内の認証プログラム３０２は、送信された認証データと使用者情報３１１（図４）の使用者４００、パスワード４０１、及び計算機情報３１２（図５）の計算機名５００、ＭＡＣアドレス５０１、ハードウェア情報５０２を比較する。使用が認められている使用者／計算機の場合は、ＭＡＣアドレス５０１とディスク情報４０２をマップ情報３１４（図６）に格納する（ステップ８０７）。また、要求元の計算機との通信データを暗号化するための鍵生成データ７００を作成し、対応するＭＡＣアドレスと作成した鍵生成データ７００を鍵データ３１３のテーブル（図７）に格納する（ステップ８０８）。また、生成した鍵生成データ７００は、使用者のハードディスク領域における鍵生成用データ２１０（図２）の格納エリアにも書き込みを行う（ステップ８０９）。鍵生成用データ２１０が書き込まれたハードディスク領域１０４にあるユーザ処理ＯＳ２００、通信処理ＯＳ２０１、複数ＯＳ処理２０２が、要求元の計算機に送信される（ステップ８１０）。

【００５１】次に、要求元の計算機は、送信された上記ＯＳ２００、２０１、２０２を起動し（ステップ８１１）、引き続き、通信処理ＯＳ２０１上で動作する通信処理、ユーザ処理ＯＳ２００上で動作するアプリケーションプログラムの順で起動処理を行う（ステップ８１２）。

【００５２】以上により、計算機上のプログラムの起動は完了する。先に述べたように、アプリケーションプログラムによるディスクに対するアクセス要求は、実施される。当該アクセス要求は図２に示す仮想ディスク処理２０７、通信処理２０５により、ハードディスク装置１００に送られ、各計算機からのハードディスクへのアクセスが実現できる。

【００５３】さらに、各計算機１１０、１２０、１３０とハードディスク装置１００間の通信データを暗号化す

る場合は、通信データの暗号化に必要な鍵生成データ２１０、７００は、上記ステップ８０８において、ハードディスク装置内にて各計算機毎に作成される。さらに、鍵生成データから鍵データが生成される。上記ステップ８１０において、図８（ｂ）のフローチャートに示すようにステップ８１０－１及び８１０－２にて、各計算機にもネットワークブート時に鍵生成データ、或いは鍵データが送信されている。そのため、図８（ａ）に示したステップ８１２の手順以降のアプリケーションプログラムによるディスクに対するアクセスに用いられる通信データを暗号化できる。

【００５４】上述した本発明の図８に示すプログラム起動手順を示すフローチャートに従い、プログラムが起動される図１のディスク装置共有システムにおいて、各計算機１１０、１２０、１３０がハードディスク装置１００を共有する方法は、以下の項目（１）から（４）の特徴を有するディスク装置の共有方法として提供可能である。

【００５５】（１）複数の計算機と、該複数の計算機により共用されるハードディスク装置と、該複数の計算機と前記ハードディスク装置がネットワークにより相互接続される計算機システムにおいて、前記計算機システムがブート処理するステップと、前記ブート処理の後、前記計算機はユーザによる認証ＩＤの入力後、認証データを作成し前記ハードディスク装置に対し、送信するステップと、前記ハードディスク装置にて前記認証データの認証処理を実施し、前記複数の計算機に対し、前記ハードディスク装置が備える暗号処理部が鍵データを作成するステップと、前記計算機の実行に必要と成るオペレーティングシステム、前記ユーザにより利用されるアプリケーションソフトと共に前記鍵データを前記計算機に対し配信するステップとを含むことを特徴とするディスク装置の共有方法。

【００５６】（２）前記ハードディスク装置は、鍵生成データ及び鍵データ部を備え、前記作成するステップにおいて、前記鍵生成データに基づいて前記鍵データが作成され、前記鍵データ部は前記複数の計算機と前記ハードディスク装置間の通信データを前記暗号処理部にて暗号化する際に必要な前記鍵データを格納することを特徴とする、上記（１）に記載のディスク装置の共有方法。

【００５７】（３）前記オペレーティングシステムは、ユーザ処理ＯＳ及び通信処理ＯＳを含み、前記配信するステップにおいて、前記計算機に対し、前記鍵生成データ或いは鍵データが前記オペレーティングシステム及びアプリケーションソフトと共に送信されることを特徴とする、上記（２）に記載のディスク装置の共有方法。

【００５８】（４）さらに前記鍵データを用いて、前記計算機は前記ユーザにより利用されるアプリケーションソフトを実行した結果、得られるデータを暗号化し前記ハードディスク装置に対し前記ネットワークを介して転送するステップを含むことを特徴とする、上記（１）に記載のディスク装置の共有方法。

【００５９】以上説明した実施形態によれば、計算機にはプログラムやデータを保存するためのハードディスクデバイスを備えることなく、ネットワーク上のハードディスク装置にプログラムやデータを保存できる。アプリケーションプログラムやＯＳなどのインストールやバージョンアップ、並びにデータのバックアップを一元管理することができる。従って運用管理コストを低減しＴＣＯの低い計算機システムを実現できるという効果がある。

【００６０】また、本実施形態によれば、一台の計算機上にＯＳを２つ搭載することによって、アプリケーションプログラムを実行するＯＳと、共有するハードディスク装置との通信処理を実行するＯＳとの機能分担を実現できる。これにより、インターネット等の外部ネットワークとハードディスク装置に対するアクセスを実現するための内部ネットワークを分離することができる。それ故、外部ネットワークから不正なプログラムにより、アプリケーションプログラムを実行するＯＳの管理者権限が奪われても、独立した通信処理を実行するＯＳが設けられる為、不正なプログラムは内部ネットワークに侵入できない。従って、共有するハードディスク装置の安全性を高めることができる。

【００６１】また、本実施形態によれば、計算機とハードディスク装置間の通信データを暗号化する場合、暗号化に必要な鍵データを生成する為のデータが、計算機をネットワークブートする段階で配布される。従って、事前に計算機に保存する必要がなく、計算機のハードウェアの解析によって、暗号化のためのデータを盗まれることがないという効果がある。ネットワークブートする段階で配布する鍵生成データは、アプリケーションプログラムを実行するＯＳから独立したもうひとつのＯＳである通信処理を実行するＯＳ側に保存することによって、外部ネットワークから不正なプログラムにより、アプリケーションプログラムを実行するＯＳの管理者権限を奪われても、鍵生成データを守ることができる。

【００６２】

【発明の効果】以上に示すように本発明に依れば、複数の計算機と共用ハードディスク装置がネットワークを介して相互接続される環境において、安全なデータ通信を実現し、計算機のメンテナンスに要する運用コストの低減を実現するディスク装置共有システムを提供する事が出来る。

【図面の簡単な説明】

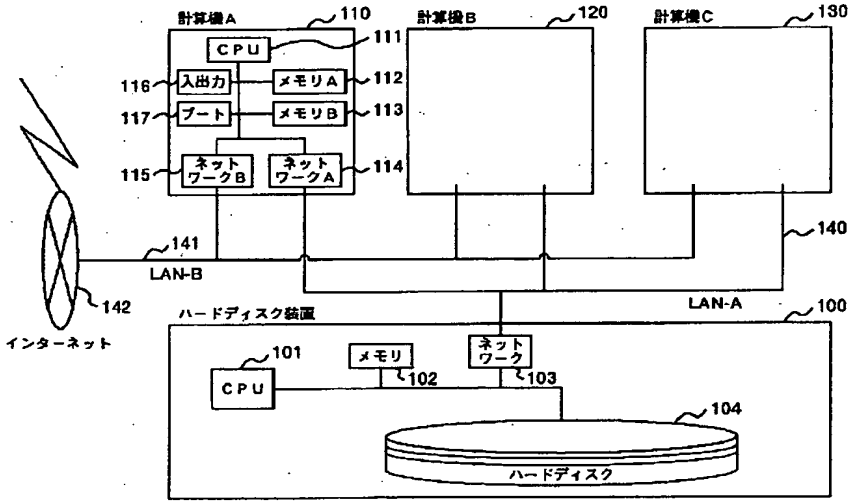
【図１】本発明の一実施例におけるディスク装置共有システムを使用した計算機環境の構成を示すシステム構成図である。

【図２】図１に示す計算機上で動作するソフトウェアの構成図である。

【図３】図１に示すハードディスク装置上で動作するソフトウェアの構成図である。
【図４】使用者情報テーブルのデータ構造を示す図である。
【図５】計算機情報テーブルのデータ構造を示す図である。
【図６】マップ情報テーブルのデータ構造を示す図である。
【図７】鍵データテーブルのデータ構造を示す図である。
【図８】図８（ａ）は、本発明の図１に示すシステム構成において計算機のブート処理手順を示すフローチャート図であり、図８（ｂ）は、図８（ａ）が示すフローチャートにおけるプログラムの転送処理の詳細フローを示す図である。
【符号の説明】
１００…ハードディスク装置、１０１…ＣＰＵ、１０２…メモリ、１０３…ネットワークデバイス、１０４…ハードディスクデバイス、１１０…計算機、１１１…ＣＰＵ、１１２…メモリ、１１３…メモリ、１１４…ネットワークデバイス、１１５…ネットワークデバイス、１１６…入出力デバイス、１１７…ブート制御回路、１２０…計算機、１３０…計算機、１４０…ネットワーク、１４１…ネットワーク、１４２…インターネット。

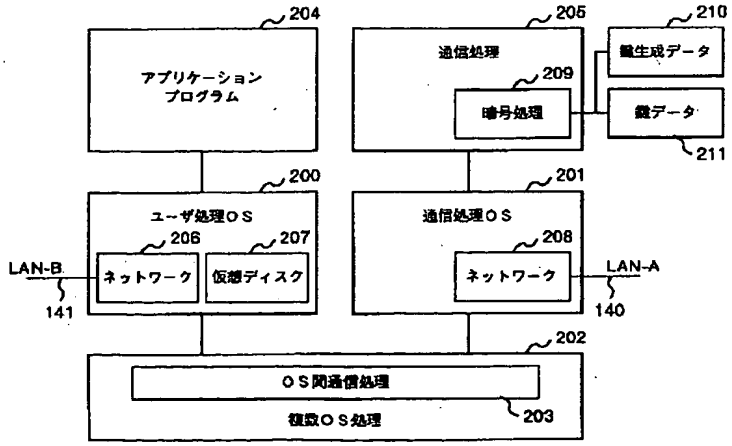
【図１】

図　1



【図２】

図　2



【図６】

図　6

314	501	402
MAC アドレス	ディスク情報	
MAC-A	DISK-A	
MAC-B	DISK-B	
MAC-C	DISK-C	

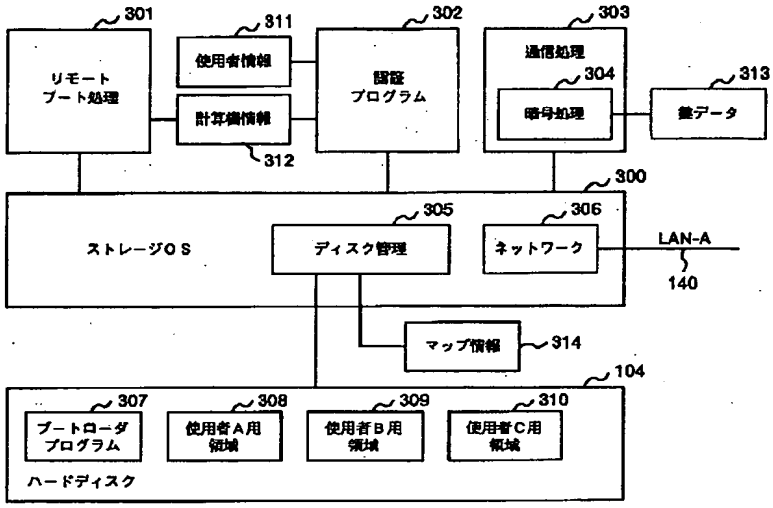
【図４】

図　4

311	400	401	402
使用者名	パスワード	ディスク情報	
使用者A	＊＊＊＊＊	DISK-A	
使用者B	＊＊＊＊＊	DISK-B	
使用者C	＊＊＊＊＊	DISK-C	

【図３】

図 3



【図５】

図 5

312

500 計算機名	501 MAC アドレス	502 ディスク情報
計算機A	MAC-A	933MH512MB
計算機B	MAC-B	733MH256MB
計算機C	MAC-C	933MH512MB

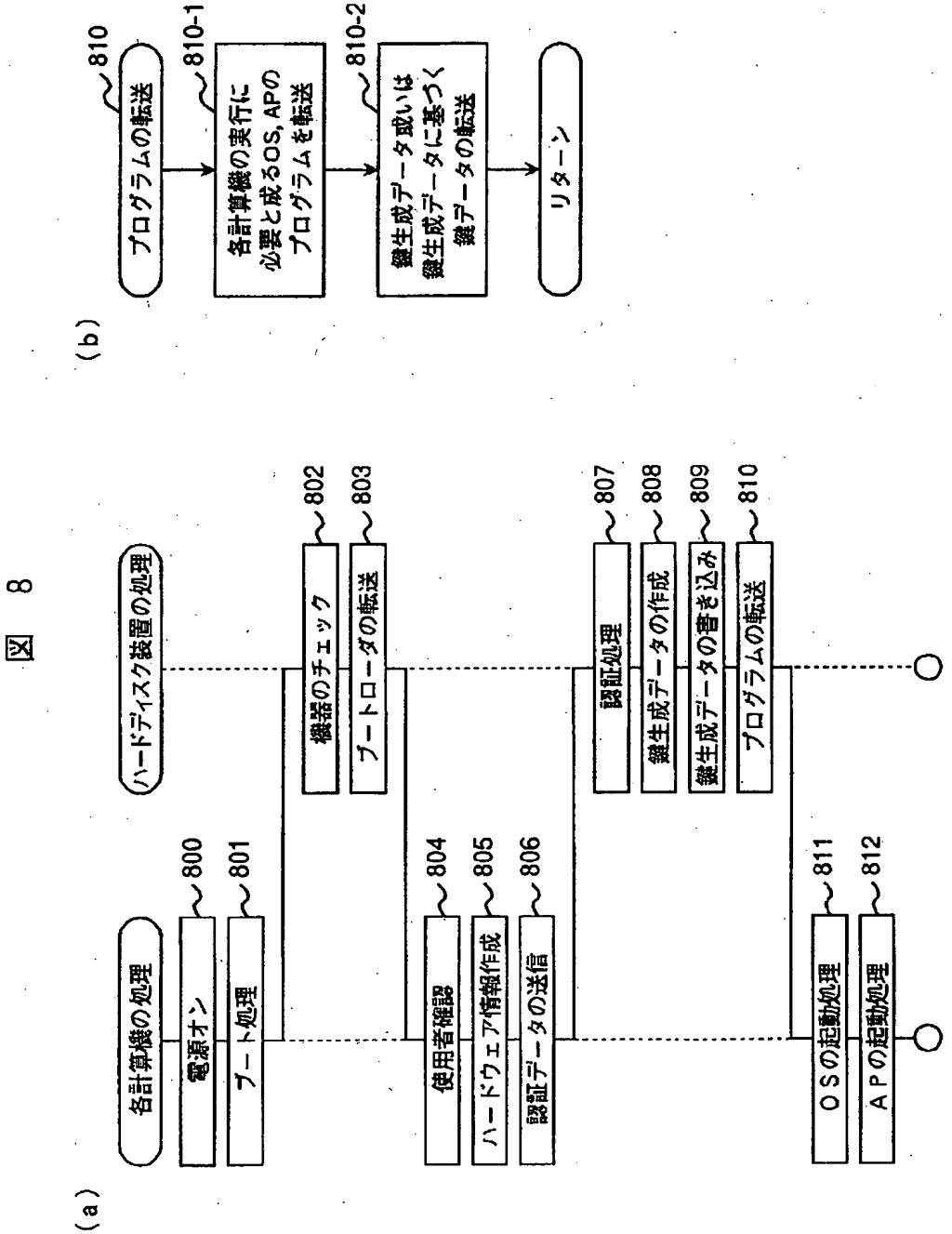
【図７】

図 7

313

501 MAC アドレス	700 鍵生成データ	701 鍵データ	702 生成時間
MAC-A	1HjzoL	＊＊＊＊＊	12:23:59
MAC-B	kOf4x	＊＊＊＊＊	10:41:12
MAC-C	uT5bq	＊＊＊＊＊	21:35:42

【図８】



フロントページの続き

(51)Int.Cl.⁷	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｈ０４Ｌ　9/10		Ｈ０４Ｌ　9/00	６２１Ａ

(72)発明者　佐藤　雅英
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　大島　訓
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考)　5B017 AA03 BA07 CA07
5B065 BA01 CA02 CC08 PA16
5B082 FA16 GA11
5J104 EA15 NA30 PA14